Director of Central Intelligence Directive no. 1/16 (1)

(2)

Security of Foreign Intelligence in Automated Systems and Networks

(Effective _____)

Pursuant to section 102 of the National Security Act of 1947, Executive Order 12356, and National Security Council (NSC) Directives, this Director of Central Intelligence Directive (DCID) establishes policy and prescribes authority and responsibilities for the protection of foreign intelligence and counterintelligence (2). derived through sensitive sources and methods and processed, stored, or communicated by automated systems or networks (3).

APPLICABILITY

This Directive applies to all United States government departments and agencies which use automated systems to process, store, or communicate intelligence information. It applies with equal force to automated systems or networks owned or operated by the United States Government and those owned or operated by contractors or consultants performing for the United States Government.

POLICY

The rapid proliferation of automated tools and methods for the electronic processing of information reinforces the requirement for providing security and surety for the intelligence information they contain and process equal to that heretofore applied to the manual and printed world. Automated systems and networks of the Intelligence Community (IC) will be managed and protected in a manner which insures that both the intelligence information and the sensitive sources and methods through which it is derived are effectively secured against successful attack by hostile intelligence activities. The goal of this Directive and the accompanying Regulation is to provide policy and broad technical guidance which will enforce the same classification, compartmentation, and need-to-know standards now applied to the manual handling of intelligence information.

The diversity and complexity of automated systems and networks now in operation in the U.S. Intelligence Community and those already designed for future installation may not provide for full compliance with the provisions of the Directive and the attached Computer Security Regulation. Therefore, the extent to which the exceptions to this Directive are applied to such systems and networks is left to the determination of each National Foreign Intelligence Board (NFIB) member in view of his ultimate responsibility for the protection of classified intelligence information.

---

1. Supercedes DCID 1/16, 6 June 1978
2. Foreign intelligence and counterintelligence are used in this directive as defined in Executive Order 12333 and as classified under the provisions of Executive Order 12356. For the purposes of this Directive, the term "intelligence information" shall include both foreign intelligence and foreign counterintelligence.
3. Automated systems and networks are defined as collections of computer-based equipment and software which are designed to process, store, or communicate information as digital data. Automated systems and networks include automated data processing (ADP),shared logic word processing (WP), automated office (AO), and electronic mail (EM) systems.

The NFIB member shall establish and maintain a formal security program to ensure adequate protection is provided for classified intelligence information processed in the community's automated systems and networks. The use of automated systems requires that classified intelligence information, when processed by computers, be afforded protection equivalent to that dictated by Presidential Policy, NSC Directives, Director of Central (DCI) Directives, and other regulations concerning the overall information security requirements, need-to-know controls, handling caveats, personnel access requirements, and dissemination procedures.

The minimum security requirements for the authorized modes of operation and the recommended criteria for determining whether the specific system or network provides the required protection is contained in the attached security regulation. The NFIB member(s) concerned may establish for specific systems or networks additional security measures and capabilities if deemed appropriate. Automated systems involving foreign governments shall be addressed on a case-by-case basis by the NFIB member(s) involved.

This Directive does not supercede or augment the requirements on the control, use, and dissemination of Restricted Data, Formerly Restriced Data, or Communications Security (COMSEC) related material as establihed by or under existing statutes, directives, or Presidential Policy.

AUTHORITY

The NFIB members are assigned the following authority concerning automated systems/network accreditations:

Automated System/Network - When an automated system or network is serving only a single NFIB member agency, the NFIB member who is the single user of the automated system/network is designated the Accreditation Authority for that system/network.

Multiple NFIB Members' System/Network - When an automated system or network is serving two or more NFIB member agencies, one NFIB member, selected by those NFIB members involved, will be designated as the Principal Accreditation Authority for that system/network.

NFIB Members' Concatenated Systems/Networks - When two or more systems/ networks are interconnected or when a system is connected to a network of systems, the NFIB members who are already designated as the Accreditation or Principal Accreditation Authority of any of the systems/networks involved will become members of the Joint Accreditation Authority for the concatenated systems/networks. One of the NFIB members of the Joint Accreditation Authority will be designated, by joint agreement, Principal Joint Accreditation Authority and all participating NFIB members shall act as a common body for executing the responsibilities of the Joint Accreditation Authority.

RESPONSIBILITIES - The NFIB member(s) serving as Accreditation Authorities are responsible to:

a. assure that compliance with stated DCI policy is accomplished in the most economical and effective operational manner.

b. Identify the information security requirements for the specific system/ network based on applicable intelligence information security policies and regulations.

c. Define the complete set of security measures/mechanisms required based on the functionality of the system/network, the user/operational environment, the information characteristics, and applicable information security criteria.

d. Perform the technical assessments, risk analyses, and security tests upon which an accreditation of the system/network can be granted.

e. Evaluate the system/network for compliance with this Directive and the requirements established in the accompanying Regulation, and certify such compliance.

f. Accredit or re-accredit the system/network and establish the allowable operational environment based on the assessment and the security tests of the system/network.

g. Coordinate all system security actions to ensure that all managers and users of an automated system or network implement the established security measures and capabilities.

EXEMPTIONS - The NFIB member or his designee may temporarily exempt specific systems under his jurisdiction from complete compliance with this Directive and the accompanying Regulation when such compliance would significantly impair the execution of his mission. An exemption shall be granted only when the NFIB member or his designee has assured himself that additional temporary measures in place will adequately protect the intelligence information being processed in the specific automated system or network.

SUPERSESSION - This Directive supersedes Director of Central Intelligence Directive No. 1/16, "Security of Foreign Intelligence in Automated Data Processing Systems and Networks", effective _____; and all existing directives, regulations, and other documents referencing the superseded Directive.

IMPLEMENTATION - Within one year of the effective date of this Directive each NFIB member will develop and promulgate a formal automated systems security program, implementing directives and regulations for systems and networks under his jurisdiction.

ADMINISTRATIVE REPORTS - Each NFIB member or his designee will provide to the DCI (attn. Chairman, Security Committee) an annual report as of 31 December detailing the accredited and exempted systems currently operating under his jurisdiction.

REVIEW - This Directive and the accompanying Regulation will be reviewed within three years from the effective date.

Next 15 Page(s) In Document Denied

Declassified in Part - Sanitized Copy Approved for Release 2012/12/18 : CIA-RDP89B01354R000600720010-6